UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/755,470	01/05/2001	Steven Branigan		4994

27997 7590 10/19/2005

PRIEST & GOLDSTEIN PLLC
5015 SOUTHPARK DRIVE
SUITE 230
DURHAM, NC 27713-7736

EXAMINER	
TRAN, ELLEN C	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/755,470	**Applicant(s)** BRANIGAN ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: 2 May 2005 with original application filed on 05 January 2001 and acknowledgement of priority established by affidavit to 01 December 2000.

2. Claims 1-15 are currently pending in this application. Claims 1, 7, and 10 are independent claims.

Response to Arguments

3. Applicant's arguments with respect to claims 1-15 have been considered but are moot in view of the new ground(s) of rejection. The Final Rejection of 28 February 2005 is replaced with this Final Office action of October 2005. The finality of this rejection is due to the amendment of the independent claims on 01 September 2004, which necessitated the new rejection as well as the affidavit submitted 2 May 2005.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

5. **Claims 1-10** are rejected under 35 U.S.C. 102(e) as being anticipated by Bahl et al. U.S. Patent No. 6,834,341 (hereinafter '341).

As to independent claim 1, "A wired network for providing secure, authenticated access to wireless network clients, comprising: a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point" is taught in '341 col. 2, line 57 through col. 3, line 25;

"the server performing authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network" is disclosed in '341 col. 12, line 24 through col. 13, line 25;

the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client" is taught in '341 col. 11, lines 35-45;

"the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client" is shown in '341 col. 13, lines 34-66;

"and a user database accessible to the server for use in validating wireless clients" is disclosed in '341 col. 12, lines 50-67.

As to dependent claim 2, "also including a network hub providing connections between the server and additional resources on the wired network" is shown in 'col. 8, lines 41-67.

As to dependent 3, **"also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network"** is disclosed in '341 col. 8, lines 41-67.

As to dependent 4, **"wherein the server is operative to provide addresses to clients through dynamic host control protocol"** is taught in '341 col. 6, line 66 through col. 7, line 3 and col. 11, lines 35-45.

As to dependent 5, **"wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol"** is shown in '341 col. 9, lines 44-50.

As to dependent 6, **"wherein the server employs 128-bit crypto-processing to communicate with the wireless network client"** is disclosed in '341 col. 14, lines 23-28.

As to independent 7, **"A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising: a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network"** is taught in '341 col. 2, line 57 through col. 3, line 25;

"the wireless network access point being further operative to receive authentication information from one or more wireless network clients" is shown in '341 col. 9, lines 33-50;

"and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and

determine if the information indicates that the wireless network client is authorized to access the wired network" is shown in '341 col. 10, lines 26-36;

"the wireless network access point being operative to receive a cryptoprocessing key from the server upon authentication of a client and to transfer the key to that client" is disclosed in '341 col. 13, lines 65-66;

"and a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network" is shown in '341 col. 12, lines 34-67;

"whether or not the wireless client is authorized to gain access to the wired network, each wireless network client being further operative to and receive address information and crypto-processing data from the network access point upon authentication by the server in order to allow communication with the wired network" is disclosed in '341 col. 11, lines 35-45 and col. 6, line 66 though col. 7, line 3;

"each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information" is taught in '341 col. 14, lines 2-9.

As to dependent 8, "wherein the access point communicates with the server using point to point tunneling protocol" is shown in '341 col. 9, lines 44-50.

As to dependent 9, "including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point

communicating with a plurality of additional wireless network clients, the wireless network access point and- the additional network access points being operative to establish connections with the server through the network hub" is disclosed in col.. 9, line 33 through col. 10, line 10.

As to independent 10, **"A method of secure communication between wireless network clients and a wired network, comprising the steps of: establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network; establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point"** is taught in '341 col. 2, line 57 through col. 3, line 25;

"exchanging encryption keys between the SB server and the wireless network client" is disclosed in '341 col. 13, line 65-66;

"transmitting authentication information from the wireless network client to the SB server through the wireless network access point; performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network" is taught in '341 col. 12, line 24 through col. 13, line 25;

"if authentication fails, rejecting connection to the wired network" is shown in '341 col. 7, lines 1-3;

"and if authentication passes, accepting connection to the wired network, providing a temporary wired network address" is disclosed in '341 col. 11, lines 35-45;

"and a unique session encryption key to the wireless network client" is taught in '342 col. 13, lines 36-40;

"and providing access to wired network resources in response to requests by the wireless network client" is shown in 'col. 8, lines 41-67.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 11-13** are rejected under 35 U.S.C. 103(a) as being unpatentable over '341 as applied to claim 10 in further view of Massarani U.S. Patent No. 6,393,484 (hereinafter '484).

As to dependent claim 11, "and wherein the step of accepting the connection is accompanied by a step of logging the acceptance" is taught in '341 col. 18, lines 33-51 "The PANS serve 302 keeps track of the number of bits that are transmitted by the user and sees that the user is billed accordingly";

the following is not taught in '341 **"wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection"** however '484 teaches "If the MAC address is not registered, the DHCP server refuses to handle the request, logs the attempt, potentially alerting network operators of a security breach" in col. 3, lines 33-51.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers taught in '341 to include a means to log rejections. One of ordinary skill in the art would have been motivated to perform such a modification to prevent unauthorized visitors see '484 (col. 1, lines 14 et seq.). "With the vast increase of private, semi-public and public shared-medium IP networks, a growing problem for network and service administrators is how to control and restrict access to the networks only to authorized and registered devices and users. One example of the problem relates to corporate IP network administrators who deal with an increasingly mobile work force that have deployed IP network access ports (typically IEEE 802.X or similar medium) throughout their corporate facilities for shared use by their corporate employees. Such shared network access ports work in conjunction with Dynamic Host Control Protocol (DHCP) servers to dynamically assign the appropriate IP address and other parameters to a mobile employee's device. A strong concern in the use of such networks is preventing visitors or unauthorized persons from taking advantage of the exposed network access ports to gain IP connectivity to the internal corporate network (intranet)".

As to dependent 12, **"wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address"** is shown in '341 col. 6, line 66 through col. 7, line 3 and col. 11, lines 35-45 "For example, an IP address might be temporarily granted to a user via a DHCP or NAT process" and "The authentication/negotiation component 110a can also include (although it is not specifically shown) a dynamic host configuration protocol (DHCP) server that is responsible for issuing and managing IP addresses. DHCP servers are known and will not be further discussed herein".

As to dependent 13, "wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol" is shown in '341 col. 9, lines 44-50 "The client can comprise any suitable computing device which, in this example, is configured for wireless communication. Each of the wireless nodes is connected through an access module 112a. In the wireless example, each access module 112a comprises one or more access points 306 that permit wireless access in known ways using known protocols".

8. **Claims 14-15** are rejected under 35 U.S.C. 103(a) as being unpatentable over '341 in further view of 484 in further view of Schuster et al. U.S. Patent No. 6,857,072 (hereinafter '072).

As to dependent 14, "wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server and wherein the authentication information is encrypted" is taught in '341 col. 12, lines 62-64 "One example of a secure link can be one that is established through the use of Secure Socket Layer (SSL) techniques. By authenticating the user in this manner, the user's authentication information is encrypted before it leaves the client machine";

the following is not taught in the '341 and '484 combination:

"using public key cryptography" however '072 teaches "One advantage of the PID-Enabled Data Network Telephony System 100 in FIG. 1 is that it may be used to provide encryption and/or authentication services. In one embodiment, the PID 110 is able to determine and exchange encryption and/or authentication data, such as a public encryption and/or authentication keys ... over a privacy network" in col. 6, lines 44-64.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify a system and method for providing network access as well as an authentication/negotiation component with service providers that also tracks rejections taught in the combination of '341 and '484 to include a means to utilize a public/private key encryption mechanism. One of ordinary skill in the art would have been motivated to perform such a modification so that sensitive data may be transmitted more securely see '072 (col. 3, lines 30 et seq.). "The present invention addresses the above needs by providing a system in a data network telephony system, such as for example, the Internet, that enables encryption and/or authentication on the telephony system. Users may participate in transactions with each other using more secure data channels. Sensitive data may be transmitted more safely across public networks"

As to dependent 15, "wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key" is taught in '341 col. 13, lines 36-40 "step 414 generates a unique token for the user. In the illustrated and described example, the PANS server 302 generates a unique token or key for each of the individual users. Step 416 then provides the user token or key to client machine for use during the user's session. Specifically, the token or key is used by the client computer each time a data packet is sent to the Internet via the PANS server 302 ... As a further added degree of security, each token or key that is used by a particular user is encrypted so that unscrupulous users cannot steal another user's token. In this example, only the client computer and the PANS server know the particular user's token or key. Any suitable encryption techniques can be used to encrypt the user's token";

"using public key cryptography" is shown in '072 col. 6, lines 44-64.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:30 am to 3:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
06 October 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100